ECE 697U - Error Control Coding, Spring 2008

Midterm Exam

Wednesday, April 2nd, 7:00-9:00pm, ELAB 327

Overview

- The exam consists of seven problems for 125 points. The points for each part of each problem are given in brackets - you should spend your **two hours** accordingly.
- The exam is closed book, but you are allowed **one page-side** of notes. Calculators are **not** allowed. I will provide all necessary blank paper.

Testmanship

- **Full credit will be given only to fully justified answers.**
- Giving the steps along the way to the answer will not only earn full credit but also maximize the partial credit should you stumble or get stuck. If you get stuck, attempt to neatly define your approach to the problem and why you are stuck.
- If part of a problem depends on a previous part that you are unable to solve, explain the method for doing the current part, and, if possible, give the answer in terms of the quantities of the previous part that you are unable to obtain.
- Start each problem on a new page. Not only will this facilitate grading but also make it easier for you to jump back and forth between problems.
- If you get to the end of the problem and realize that your answer must be wrong (e.g. the Fourier Transform of a real signal that is not conjugate symmetric), be sure to write "this must be wrong because . . . " so that I will know you recognized such a fact.
- Academic dishonesty **will** be dealt with **harshly** - the *minimum penalty* will be an "F" for the course.

1. A stream of independent information bits, each equally likely to be 0 or 1, are grouped to form row vectors $\underline{u}$ of length 3, which are used by the channel encoder to form codewords by $\underline{u}G$, where

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Note: **Nowhere in this problem do you need to construct the standard array, so do not waste time doing so!**

[10] (a) Each part is worth two points, and **no justification is required**.

- What is the rate r of this code ?
- Give the set of codewords $\mathcal{C}$.
- Give the parity check matrix H of the code.
- How many syndromes are there?
- Is this code cyclic?

[5] (b) Does this code have the largest minimum (Hamming) distance of any (7,3) linear block code?

[5] (c) List the syndromes with the coset leaders corresponding to each syndrome.

[5] (d) Consider a binary sequence $\underline{x}$ of length 7 that is chosen so as to maximize the Hamming distance between $\underline{x}$ and the nearest codeword (i.e. $\underline{x}$ is chosen as far away from the code as possible). How far (in Hamming distance) is $\underline{x}$ from the nearest codeword?

[10] (e) Suppose I am transmitting the coded bits over a binary symmetric channel (BSC), and at the receiver I want to **simultaneously** correct all error patterns of weight less than two and detect all error patterns of weight two. (In other words, if the error pattern has weight zero or one, I want to output the correct codeword. If the error pattern has weight two, I want to indicate that there is more than one error.)

Give an **algorithm** that performs this error correction/detection. This algorithm should start with the length 7 vector $\underline{y}$ that is output from the BSC.

2. [5](a) Consider the following syndromes with their associated coset leaders:

$\underline{s}$	Coset Leader
000	00000
001	10000
010	01000
011	00011
100	00100
101	00010
110	00001
111	10001

Does a linear block code exist with this syndrome to coset leader mapping? If your answer is "yes", give **any one of the following:** the code's generator matrix, parity check matrix, **or** codewords. If your answer is "no", explain why such a code does not exist?

[5](b) Consider the following syndromes with their associated coset leaders:

$\underline{s}$	Coset Leader
000	00000
001	00001
010	00010
011	00100
100	01000
101	10000
110	11000
111	10001

Does a linear block code exist with this syndrome to coset leader mapping? If your answer is "yes", give **any one of the following:** the code's generator matrix, parity check matrix, **or** codewords. If your answer is "no", explain why such a code does not exist?

3. A popular construction in coding theory is the $|u|u+v|$ construction. A $(2n, k)$ code $\mathcal{C}$ is defined from an (n, k_1) linear block code $\mathcal{C}_1$ and an (n, k_2) linear block code $\mathcal{C}_2$ as:

$$\mathcal{C} = \{|u|u \oplus v| : u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$$

where $|x|y|$ stands for the concatenation of strings x and y. **For example**, if $x = 11010$ and $y = 00001$, then $|x|y| = 1101000001$. Thus, the code $\mathcal{C}$ consists of *all* concatenations $|u|u \oplus v|$ such that u is a codeword from $\mathcal{C}_1$ and v is a codeword from $\mathcal{C}_2$. **For example,** if $\mathcal{C}_1$ has four codewords and $\mathcal{C}_2$ has eight codewords, then $\mathcal{C}$ will have 32 codewords.

[5] (a) Show that $\mathcal{C}$ is a linear code.

[10] (b) Suppose the minimum Hamming distance of $\mathcal{C}_1$ is d_1 and the minimum Hamming distance of $\mathcal{C}_2$ is d_2. Show that the minimum Hamming distance of $\mathcal{C}$ is given by the minimum of $2d_1$ and d_2 by showing:

(i) If $v = 0$, the minimum weight of a constructed codeword is greater than or equal to $2d_1$.

(ii) If $v \neq 0$, the minimum weight of a constructed codeword is greater than or equal to d_2.

4. The polynomial $X^5 + X^3 + X^2 + X + 1$ is primitive over the binary field.

   [15] (a) Use the polynomial give above to construct $GF(32)$.

   [5] (b) Write down the cyclotomic cosets (use exponent notation).

   [10] (c) Given that $X^5 + X^2 + 1$ and $X^5 + X^4 + X^2 + X + 1$ are irreducible polynomials over the binary field, find the minimum polynomials of each of the cyclotomic cosets.

   [5] (d) Find the rate of a $(31, k)$ four-error correcting (strict-sense) BCH code of maximum rate.

5. [10] **Justify your answers for each of the below from first principles!**

   (a) How many polynomials of degree 2 with coefficients in the binary field are irreducible?

   (b) How many polynomials of degree 4 with coefficients in the binary field are irreducible?

   (c) How many polynomials of degree 8 with coefficients in the binary field are irreducible?

6. [10] Prove the following statement: If $m_\alpha(X)$ is the minimum polynomial of the primitive element used to construct $GF(2^m)$, the BCH code with $g(X) = m_\alpha(X)$ is a Hamming code. Recall that a Hamming code is defined as a linear block code with a parity check matrix whose columns consist of all non-zero binary m-tuples.

7. [10] Consider an (N, K) Reed-Solomon code where $N = q - 1$ that works with $q - ary$ symbols (where $q = 2^m - 1$). Suppose that you were to write out (in bits) all of the "guaranteed" correctable error patterns; i.e., those with *symbol* weight less than

$$\left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor .$$

   - What is the maximum binary weight of an error pattern in the "guaranteed" correctable error pattern list ?
   - What is the minimum binary weight of an error pattern that falls outside the "guaranteed" correctable error pattern list ?